

REMARKS/ARGUMENTS

The Office Action mailed August 24, 2006 has been carefully considered.
Reconsideration in view of the following remarks is respectfully requested.

The Status of the Claim

Claims 3, 6, 9-15, 17-39 and 42-63 are now pending. No claims stand allowed.

The 35 U.S.C. §103 Rejection

Claims 3, 6, 9-13, 18, 20, 24-25, 27-34, 39, 42-43, 45, 47-49, 51, 53-54, 56 and 60 stand rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Shen (E.P.No. 1,074,949) in view of Beatson et al. (U.S. Pat. No. 5,892,824) and/or McPillie et al. (UK Pat. Application No. GB 2 2336 005 A), among which claims 3, 30, 39, 45, 53, and 54 are independent claims. This rejection is respectfully traversed.

According to M.P.E.P. §2143,

To establish a *prima facie* case of obviousness, three basic criteria must be met. First there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in the applicant's disclosure.

Furthermore, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990).

Regarding Claims 3, 39, and 53:

Claim 3 defines an intelligent identification card comprising (a) an on-board memory for storing reference data, (b) an on-board sensor for capturing live biometric data, (c) an on-board microprocessor for comparing the captured biometric data with corresponding stored reference data within a predetermined threshold and for generating a verification message only if there is a match within a predetermined threshold, and (d) an interface for communicating the verification message to an external network, wherein the verification message includes at least excerpts from the captured biometric data, the verification message being transmitted to a remote authentication system for additional verification using reference data which is different from the reference data stored on said on-board memory, as recited in claim 3.

In the Final Office Action, the Examiner specifically contends that the elements of the presently claimed invention are disclosed in Shen except that Shen does not teach the verification message including at least excerpts from the captured biometric data, the verification message being transmitted to a remote authentication system for additional verification using reference data which is different from the reference data stored on said on-board memory. The Examiner further contends, however, that Beatson teaches the verification message including at least excerpts from the captured biometric data, the

verification message being transmitted to a remote authentication system for additional verification using reference data which is different from the reference data stored on said on-board memory (citing column 6, lines 39-45 of Beatson), and that it would have been obvious to one having ordinary skill in the art at the time of the invention to incorporate Beatson into Shen because the supplied biometric data is used to determine if the identity of the user is verified and provides an audit trail of actual users. Claims 39 and 53 also stand rejected in a similar manner.

The Applicants respectfully disagree for the reasons set forth below.

Beatson relates to systems and methods for handling and processing handwritten signatures. In Beatson, a verification template for the cardholder's signature is stored on a smart IC card, along with an image of the signature for visual comparison. When a user signs on the spot, the signature is electronically captured, and the signature terminal carries out the signature verification analysis by comparing the captured signature with the verification template read out from the smart IC card (column 5, lines 22-62 of Beatson). If the signature is accepted by the signature terminal, the verification template is updated based on the previous template and the last good signature (column 6, lines 7-16 of Beatson). This is because the signature is a "behavioral" biometric which may change over time, as opposed to a physical biometric, such as a fingerprint (column 4, lines 43-47 of Beatson), which is typically an unchanging, permanent record.

In the portion (column 6, lines 39-45) cited by the Examiner, Beatson states as follows:

A means of two-way communication with a host device so that a signature captured electronically may be compared with that stored on the smart card or at the host device and may be communicated to the host together with the result of the signature comparison for display, storage, onward transmission or hard copy reproduction (emphasis added).

Accordingly, Beatson only suggests that an electronically captured signature may be compared with that stored at the host device as an alternative to the on-card comparison, not as an additional verification. If the captured signature is sent to the host together with the on-card verification result, it is sent only for display, storage, onward transmission or hard copy reproduction, not for additional verification process (see the above citation). That is, Beatson only teaches performing an on-card verification, and alternatively, not additionally, performing a verification process at the host device. In addition, there is no mention or suggestion in Beatson that the host device has a verification template (the alleged reference data) which is different from the verification template stored on the smart IC card.

Furthermore, Beatson states as follows (column 6, lines 46-49 thereof):

A method of comparing a submitted signature against a signature verification template supplied from the host or from a smart card based upon the extraction of a number of mathematically defined features (emphasis added).

Again, Beatson only suggest using the verification template from the host or the smart card as an alternative, not the both.

Accordingly, Beatson fails to teach or suggest the claimed verification message transmitted to a remote authentication system for additional verification using reference data which is different from the reference data stored on said on-board memory, as recited in claim 1.

Regarding Claims 30, 45, and 54:

Claim 30 defines an intelligent identification card comprising (a) an on-board sensor for capturing live biometric data, (b) a first on-board processor coupled with said on-board sensor, said first on-board processor including a memory storing reference data, said first on-board processor comparing the captured biometric data with corresponding stored reference data within a predetermined threshold and generating a verification message only if there is a match within a predetermined threshold, (c) a second on-board processor coupled with said first on-board processor, for executing intelligent card functions, the verification message enabling said second on-board processor, and (d) an interface coupled to either one of said first on-board processor and said second on-board processor, for communicating with an external network, as recited in claim 30.

In the Final Office Action, the Examiner specifically contends that the elements of the presently claimed invention are disclosed in Shen except that Shen does not teach a second on-board processor coupled with the first on-board processor, for executing intelligent card functions, the verification message enabling said second on-board processor. The Examiner further contends, however, that McPhillie teaches a second on-board processor coupled with the first on-board processor, for executing intelligent card

functions (citing FIG. 4, box 119 thereof), the verification message enabling said second on-board processor (citing page 5, lines 3-22 thereof), and that it would be obvious to one having ordinary skill in the art at the time of the invention to incorporate McPhillie into Shen because utilizing a second co-processor for a specific purpose makes the processor faster. Claims 45 and 54 also stand rejected in a similar manner.

The Applicants respectfully disagree for the reasons set forth below.

In Shen, the processing unit (14) verifies the user by comparing the received fingerprint scan data with the stored fingerprint reference data, and activates the card reader interface (13) if the user is verified (see Abstract thereof). As the Examiner correctly noted, Shen's card has only one processor.

McPhillie allegedly discloses two processor system for a development tool (Emulation Module Interface (EMI) 40), which allegedly includes a first (unsecure) processor 44 without access to the cryptographic functions, and a second (secure) processor 46 having the full cryptographic functions (page 5, lines 5-17, FIG. 4 thereof). As discussed in Applicant's previous response, however, the unsecure processor 44 and the secure processor 46 are two versions (or "copies") of the same integrated circuit (IC) 100 to emulate the functions thereof. The name "secure" in McPhillie simply means that the emulation includes the cryptographic function, and the name "unsecure" simply means that the emulation dose not include the cryptographic function. That is, McPhillie's alleged "secure" and "unsecure" processors perform (or emulate) the same

functions of the original smartcard processor 110, except that the “unsecure” processor lacks the cryptographic function. McPhillie does not teach or suggest that the unsecure processor 44 is enabled or activated by a verification message generated by the secure processor 46 or any other verification message. Therefore, contrary to the Examiner’s allegation, McPhillie fails to teach or suggest the claimed second on-board processor coupled with said first on-board processor, for executing intelligent card functions, the verification message enabling said second on-board processor, as recited in claim 30.

It should be noted that the Examiner’s allegation that “the claim calls for a card that contains two processors, one of which being secure” and “[t]his is taught by figures in McPhillie” is incorrect. Claim 30 does not simply call for a card including two processors one of which is named “secure.” As discussed above, claim 30 clearly recites specific and different operations of the respective processors, and the operational relationship therebetween that the verification message generated by the first processor enables the second processor.

Thus, even if McPhillie’s teaching should be combined with Shen, the alleged combination would provide another version/copy of Shen’s processor 14 which lacks a particular (cryptographic) function but otherwise the same. Shen’s processor 14 would still perform the fingerprint matching and then activate the card reader interface 13, not the alleged second processor allegedly taught by McPhillie. This is because none of Shen or McPhillie teaches or suggests enabling one processor by a verification message generated by the other.

Accordingly, Shen, whether considered alone or combined with or modified by McPhillie, does not teach an intelligent identification card comprising, among others, a first on-board processor coupled with said on-board sensor, said first on-board processor including a memory storing reference data, said first on-board processor comparing the captured biometric data with corresponding stored reference data within a predetermined threshold and generating a verification message only if there is a match within a predetermined threshold, and a second on-board processor coupled with said first on-board processor, for executing intelligent card functions, the verification message enabling said second on-board processor, as recited in claim 30.

Claims 45 and 54 include substantially the same distinctive features as claim 30.

Accordingly, it is respectfully requested that the rejection of claims based on Shen and McPhillie be withdrawn. In view of the foregoing, it is respectfully asserted that the claims are now in condition for allowance.

Dependent Claims

Claims 6, 9-15, and 17-29 depend from claim 3, claims 31-38 and claims 56-59 depend from claim 30, claims 42-44 depend from claim 39, claims 46-52 and claims 60-63 depend from claim 45, and claim 55 depends from claim 54, and thus include the limitations of the corresponding independent claims. The argument set forth above is

equally applicable here. The base claims being allowable, the dependent claims must also be allowable at least for the same reasons.

In view of the foregoing, it is respectfully asserted that the claims are now in condition for allowance.

Conclusion

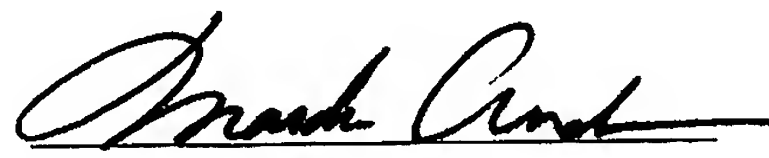
It is believed that this Amendment places the above-identified patent application into condition for allowance. Early favorable consideration of this Amendment is earnestly solicited.

If, in the opinion of the Examiner, an interview would expedite the prosecution of this application, the Examiner is invited to call the undersigned attorney at the number indicated below.

The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 50-1698.

Respectfully submitted,
THELEN REID & PRIEST, LLP

Dated: October 24, 2006


Masako Ando
Ltd. Rec. No. L0016

Thelen Reid & Priest LLP
P.O. Box 640640
San Jose, CA 95164-0640
Tel. (408) 292-5800
Fax. (408) 287-8040